DPIA PER IL SISTEMA DI SORVEGLIANZA "BODY-CAM" PER IL PERSONALE DELLA POLIZIA MUNICIPALE

AUTORE :
ISPETTOR FRANCESCO MODICA Di MARCO

REVISORE:
Avvocato Nadia CORA'

VALIDATORE :
Ispettor Francesco MODICA DI MARCO

Mappaggio dei rischi

Principi fondamentali

Misure esistenti o pianificate

Rischi - Accesso illegittimo ai dati

Piano d'azione / misure correttive :
i rischi legati ai possibili accessi illegittimi ai dati saranno di volta in volta valutati in modo da intraprendere delle misure correttive tali da garantire la sicurezza della conservazione ed integrità dei dati.
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?
Limitata
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?
Limitata

Rischi - Modifiche indesiderate dei dati

Piano d'azione / misure correttive :
i rischi inerenti alle eventuali modifiche o alterazioni verranno di volta in volta valutati in modo da applicare in ogni momento misure correttive per garantire la sicurezza della gestione e del trattamenti dei dati
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?
Importante
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?
Trascurabile

Rischi - Perdita di dati

Piano d'azione / misure correttive :
gli eventuali rischi della perdita dei dati saranno di volta in volta valutati in modo da avere un continuo aggiornamento e miglioramento delle misure correttive a garanzia della sicurezza
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? **Importante**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)? **Limitata**

Nome del DPO/RPD

Avvocato Nadia CORA'

Posizione del DPO/RPD

Il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

La base giuridica del trattamento, ai sensi dell'articolo 6, paragrafo 1, lettera "e" del GDPR (Reg. UE 679/2016), è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per tale motivo all'insorgere di rischi legati a tale possibile scenario, l'uso delle body-cam risulta essere legittimato e pertanto non è necessario richiedere il parere degli interessati che comunque saranno avvertiti al momento dell'utilizzo dei dispositivi.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Sistemi di ripresa audio/video indossabili in dotazione al Comando di Polizia Municipale di Campo nell'Elba da utilizzare al verificarsi di tangibili situazioni di pericolo, di turbamento dell'ordine e della sicurezza pubblica, in caso di pericolo imminente per persone e/o cose, nell'ambito delle finalità dell'accertamento e delle repressione dei reati e in relazione all'evolversi degli scenari di sicurezza e di ordine pubblico che facciano presupporre, a suo giudizio, situazioni di criticità. Costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Municipale svolge quotidianamente nell'ambito delle proprie competenze istituzionali sul territorio comunale, in stretto raccordo con le altre Forze dell'Ordine. Attraverso tali strumenti si persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, paesaggistico, artistico e culturale, negli edifici pubblici, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare, sui lungomare ed in prossimità delle spiagge, specialmente nel periodo di maggiore affluenza turistica.

Il sistema può essere attivato dal singolo operatore, in relazione all'evolversi degli scenari di sicurezza o che facciano presupporre una criticità o un dovere istituzionale tali da richiedere una assoluta tempestività dell'iniziativa. L'operatore di polizia potrà altresì attivare la registrazione per attività di indagine di Polizia Giudiziaria nonché nella flagranza di reato o comunque di concreto pericolo di danno a persone e cose, desumibile dalle circostanze. Dovrà adottare particolari cautele nel caso in cui le riprese video possano riprendere luoghi assistiti da particolari aspettative di riservatezza come nel caso di scuole, luoghi di culto, di cura, di strutture ospedaliere nonché in presenza di soggetti vulnerabili, quali minori e vittime di reati particolarmente gravi ovvero in situazioni in cui possono essere trattati particolari categorie di dati personali. E' tenuto, inoltre, ad avvisare i presenti che sta effettuando una registrazione audiovisiva. **L'accesso alle immagini da parte del Responsabile e degli incaricati del trattamento dei dati si limita alle attività oggetto della sorveglianza, eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione. Nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal Responsabile e dagli incaricati del trattamento dei dati. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate. Le operazioni di cancellazione devono essere effettuate esclusivamente sul luogo di lavoro. L'accesso alle immagini ed ai dati personali è consentito:**
- al Responsabile ed agli incaricati dello specifico trattamento;
- ai preposti alle indagini dell'Autorità Giudiziaria o di Polizia;
- all'Amministratore di Sistema del Comune di Campo nell'Elba e alla ditta fornitrice delle apparecchiature nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione. L'interessato potrà esercitare i propri diritti nelle modalità previste dalla relativa normativa e tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo od informatico), conservato nell'Ufficio della Polizia Municipale, nel quale sono riportati ad opera degli incaricati:

- la data e l'ora dell'accesso;

- l'identificazione del terzo autorizzato;

- i dati per i quali si è svolto l'accesso;

- gli estremi e la motivazione dell'autorizzazione all'accesso;

- le eventuali osservazioni dell'incaricato;

- la sottoscrizione del medesimo.

Ci sono standard applicabili al trattamento?

Il Comune di Campo nell'Elba nella persona del Sindaco pro-tempore (o suo delegato) è titolare del trattamento dei dati personali acquisiti mediante l'utilizzo delle microcamere. **Il Responsabile dell'Ufficio di Polizia Municipale di Campo nell'Elba assume la responsabilità del trattamento dei dati personali rilevati, sul quale gravano i doveri di vigilanza e di adozione delle precauzioni**. Incaricati del trattamento e quindi autorizzati ad utilizzare ed a visionare le registrazioni, nei casi in cui sia indispensabile per gli scopi perseguiti, sono i soggetti indicati dal Responsabile del trattamento dei dati rilevati, in servizio presso l'Ufficio di Polizia Municipale del Comune di Campo nell'Elba

I dati personali oggetto di trattamento devono essere:

-trattati in modo lecito e secondo correttezza, effettuati con i sistemi di ripresa in questione e rispettare i principi espressi dal D.Lgs. 30 giugno 2003, n. 196 così come modificato dal D.Lgs. 101//2018, nonché dal Reg. UE 27 aprile 2016, n. 2016/679/UE (cd. GDPR) e dal D.Lgs. 18 maggio 2018, n. 51;

- essere pertinenti, completi e non eccedenti le finalità per le quali risultano essere raccolti, ovvero successivamente trattati, nonché conservati per un periodo non superiore a 7 giorni in una forma che consenta l'identificazione dell'interessato fatte salve speciali esigenze di ulteriore conservazione. Al termine del tempo stabilito le riprese dovranno essere cancellate;

- trattati, con riferimento alla finalità di cui al precedente articolo 1, commi 1,2 e 3, con modalità rivolte a salvaguardare l'anonimato anche successivamente alla fase della raccolta, atteso che tali immagini registrate potrebbero contenere dati di carattere personale.

I trattamenti di cui al D.Lgs 51/2018 debbono rispettare i principi di cui agli articoli 5-6 GDPR; tra questi, in particolare, quelli secondo cui i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato.

In caso di registrazione di riprese in occasione di situazioni di presunto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, le immagini stesse dovranno essere tempestivamente cancellate, in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui al Decreto Legislativo 51/2018.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Premesso che il sistema NON INTEGRA dispositivi tecnici diretti a consentire l'identificazione univoca o l'autenticazione di una persona fisica (facial recognition), i dati personali oggetto di trattamento devono essere:

-trattati in modo lecito e secondo correttezza, effettuati con i sistemi di ripresa in questione e rispettare i principi espressi dal D.Lgs. 30 giugno 2003, n. 196 così come modificato dal D.Lgs. 101//2018, nonché dal Reg. UE 27 aprile 2016, n. 2016/679/UE (cd. GDPR) e dal D.Lgs. 18 maggio 2018, n. 51;

- essere pertinenti, completi e non eccedenti le finalità per le quali risultano essere raccolti, ovvero successivamente trattati, nonché conservati per un periodo non superiore a 7 giorni in una forma che consenta l'identificazione dell'interessato fatte salve speciali esigenze di ulteriore conservazione. Al termine del tempo stabilito le riprese dovranno essere cancellate;

- trattati con modalità rivolte a salvaguardare l'anonimato anche successivamente alla fase della raccolta, atteso che tali immagini registrate potrebbero contenere dati di carattere personale.

I trattamenti di cui al D.Lgs 51/2018 debbono rispettare i principi di cui agli articoli 5-6 GDPR; tra questi, in particolare, quelli secondo cui i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato. In caso di registrazione di riprese in occasione di situazioni di presunto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, le immagini stesse dovranno essere tempestivamente cancellate, in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui al Decreto Legislativo 51/2018.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I segnali video delle unità di ripresa saranno trasferiti direttamente su server locale dedicato oppure su piattaforma cloud, crittografate per permetterne la conservazione a norma. Le immagini

videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti consentiti dalla Legge, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.
Al termine del servizio ciascun operatore dovrà consegnare la telecamera al Responsabile del trattamento dati in modo da poter scaricate le immagini eventualmente registrate dall'operatore, provvedendo ad annotare nell'apposito registro l'ora di inserimento della microcamera nella docking station.

Il settore di ripresa delle microcamere potrà essere operativo nei luoghi pubblici o aperti al pubblico, con esclusione delle proprietà private (salvo i casi di flagranza di reato).

Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati nel limite del tempo ammesso per la loro conservazione e solo in caso di effettiva necessità di ulteriori indagini per il conseguimento delle finalità perseguite a norma di Legge.

In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale o del patrimonio pubblico, il Responsabile o l'incaricato provvederà a darne comunicazione senza ritardo all'Autorità competente, garantendo al contempo la conservazione dei dati delle immagini su appositi supporti.

Alle immagini raccolte ai sensi del presente articolo possono accedere, per l'espletamento delle relative indagini, solo gli appartenenti all'Amministrazione Giudiziaria o le persone da essi espressamente autorizzate e gli organi di Polizia.

Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino una copia delle riprese effettuate, devono presentare un'istanza scritta e motivata indirizzata al Responsabile della gestione e del trattamento dei dati.

Quali sono le risorse di supporto ai dati?

Le microcamere hanno una risoluzione Full HD 1080P (60/30 fps), consentono la registrazione fino a 12 ore con un'autonomia della batteria di circa 12 ore. Il campo visivo è di 130° e consentono l'archiviazione di 64 Gb in formato video MP4 (H.264).
Le microcamere consentono, tecnicamente, riprese video diurne/notturne a colori in condizioni di sufficiente illuminazione naturale o artificiale.

Ogni body-cam è provvista di un sistema di buffering "pre-evento" che permette la registrazione dell'evento a partire da 2 minuti prima della messa in funzione delle microcamere stesse.

I segnali video delle unità di ripresa saranno trasferiti direttamente su server locale dedicato oppure su piattaforma cloud, crittografate per permetterne la conservazione a norma. Le immagini videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite dalla Legge, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.

I dati sono protetti da idonee e preventive misure di sicurezza, individuate con documentazione tecnica rilasciata dalla Ditta produttrice, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Saranno comunque assicurate misure adeguate ai sensi dell'articolo 32 GDPR. I dati personali oggetto di trattamento sono custoditi in un server dedicato posto presso l'Ufficio di Polizia Municipale del Comune di Campo nell'Elba, in un luogo chiuso al pubblico, possono accedere esclusivamente il Responsabile e gli incaricati del trattamento dei dati. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati.
Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La base giuridica del trattamento, ai sensi dell'articolo 6, paragrafo 1, lettera "e" del GDPR (Reg. UE 679/2016), è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
Valutazione :
Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Attraverso tali strumenti si persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, paesaggistico, artistico e culturale, negli edifici pubblici, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare, sui lungomare ed in prossimità delle spiagge, specialmente nel periodo di maggiore affluenza turistica. L'utilizzo è giustificato in caso di effettiva necessità al verificarsi di tangibili situazioni di pericolo, di turbamento dell'ordine e della sicurezza pubblica, in caso di pericolo imminente per persone e/o cose, nell'ambito delle finalità dell'accertamento e delle repressione dei reati e in relazione all'evolversi degli scenari di sicurezza e di ordine pubblico che facciano presupporre, a suo giudizio, situazioni di criticità.
Valutazione :
Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I trattamenti di cui al D.Lgs 51/2018 rispettano i principi di cui agli articoli 5-6 GDPR; tra questi, in particolare, quelli secondo cui i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato.

Valutazione :

Accettabile

I dati sono esatti e aggiornati?

I dati sono protetti da idonee e preventive misure di sicurezza, individuate con documentazione tecnica rilasciata dalla Ditta produttrice, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

I dati personali oggetto di trattamento sono custoditi in un server dedicato posto presso l'Ufficio di Polizia Municipale del Comune di Campo nell'Elba, in un luogo chiuso al pubblico, possono accedere esclusivamente il Responsabile e gli incaricati del trattamento dei dati. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati.

Valutazione :

Accettabile

Qual è il periodo di conservazione dei dati?

Le immagini videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.

Valutazione :

Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'operatore ha l'obbligo di avvisare i presenti che sta effettuando una registrazione a registrazione audio/video, ogniqualvolta si presenti il realizzarsi di eventi per i quali sia reso lecitol'utilizzo del sistema di sorveglianza previsto dalla Normativa ai sensi dell'articolo 6, paragrafo 1, lettera "e" del GDPR (Reg. UE 679/2016), rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Valutazione :
Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?
nello specifico la base giusridica riferita allo strumento oggetto della presente DPIA non prevede alcun consenso degli interessati.

Valutazione :
Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

All'interessato, relativamente al trattamento dei suoi dati personali, sono riconosciuti i seguenti diritti:

- richiedere maggiori informazioni in relazione ai contenuti dei verbali amministrativi;
- diritto di accesso ai dati personali (art.15 GDPR);
- diritto di rettifica dei dati personali senza ingiustificato ritardo (art.16 GDPR);
- diritto alla cancellazione dei dati. La cancellazione non è consentita per i dati contenuti negli atti che devono obbligatoriamente essere conservati dal Titole (art.17 GDPR);
- diritto di limitazione del trattamento (art.18 GDPR);
- diritto alla portabilità dei dati (art.20 GDPR);
- diritto di opposizione (art.21 GDPR);

- diritto relativo al processo decisionale automatizzato, compresa la profilazione (art.22 GDPR);
- diritto di proporre reclamo al Garante per la protezione dei dati personali (art.77 GDPR);

Ogni interessato ha la facoltà di far valere i propri diritti riconosciuti dalla Legge a seguito del realizzarsi di un evento da cui possa essere necessario, per motivi di giustizia, l'avvio di un procedimento di cui verrà reso edotto.
Valutazione :
Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Ogni interessato ha la facoltà di far valere i propri diritti riconosciuti dalla Legge a seguito del realizzarsi di un evento da cui possa essere necessario, per motivi di giustizia, l'avvio di un procedimento di cui verrà reso edotto.
Valutazione :
Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

all'interessato viene garantito il diritto alla limitazione del trattamento dei dati (art.18 del GDPR) e all'opposizione (art.21 del GDPR), con le modalità previste dalla Legge nel momento del concretizzarsi di un evento da cui possa essere necessario, per motivi di giustizia, l'avvio di un procedimento di cui verrà reso edotto.
Valutazione :
Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del responsabile del Trattamento dei dati sono dettati nel Decreto di nomina del Sindaco di Campo nell'Elba e dai contratti e le convenzioni con i concessionari per la gestione del ciclo contravvenzionale.
Valutazione :
Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Gli atti amministrativi relativi alle violazioni da parte di cittadini residenti fuori dall'UE vengono trattati con la medesima protezione di quelli residenti all'interno della UE.
Valutazione :
Accettabile

Misure esistenti o pianificate

Rischi

Crittografia

I segnali video delle unità di ripresa saranno trasferiti direttamente su server locale dedicato oppure su piattaforma cloud, crittografate per permetterne la conservazione a norma. Le immagini videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.

Valutazione :

Accettabile

Tracciabilità

Al termine del servizio ciascun operatore dovrà consegnare la telecamera al Responsabile del trattamento dati in modo da poter scaricate le immagini eventualmente registrate dall'operatore, provvedendo ad annotare nell'apposito registro l'ora di inserimento della microcamera nella docking station. Tali immagini saranno conservate solo ed esclusivamente per scopi compatibili alle finalità per le quali è consentito l'utilizzo delle body-cam, come indicato in premessa nella presente DPIA, e solamente per il periodo necessario e/o eventualmente richiesto dall'AG. Il Responsabile dela Trattamento dei dati avrà cura di cancellare le immagini al termine del periodo consentito al trattamento dei dati, annotando l'operazione sull'appostito registro di consegna del dispositivo.

Valutazione :

Accettabile

Archiviazione

Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati nel limite del tempo ammesso per la loro conservazione e solo in caso di effettiva necessità di ulteriori indagini.

Le immagini videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.

Valutazione :

Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati e archiviati nei locali indisponibili all'utenza dell'ufficio di Polizia Municipale e quelli inutilizzabili vengono distrutti con appositi macchinari tritacarte.

Valutazione :

Accettabile

Vulnerabilità

I software utilizzati per la trasmissione dei dati sono costantemente aggiornati. I filmati e le immagini possono essere visionati solo con l'ausilio di un software licenziato e le apparecchiature sono soggette a revisione periodica.

Valutazione :

Accettabile

Lotta contro il malware

I sistemi informatici sono protetti dal malware con modalità di protezione sia hardware che software (antivirus).

Valutazione :

Accettabile

Gestione postazioni

La postazione presente presso l'ufficio di Polizia Municipale è dotata di PC con relativa password alfanumerica che viene modificata periodicamente al fine di garantire un accesso sicuro.

Valutazione :

Accettabile

Backup

Il backup dei dati trattati avviene periodicamente ed in modo automatico su disco fisso.

Valutazione :

Accettabile

Manutenzione

La manutenzione dei sistemi è stata affidata a Ditta specializzata tramite affidamento effettuato a norma di legge.

Valutazione :

Accettabile

Controllo degli accessi fisici

L'accesso al server è consentito solo al personale autorizzato.

Valutazione : Accettabile

Sicurezza dell'hardware

Il server è ubicato presso i locali indisponibili all'utenza dell'ufficio di Polizia municipale e l'accesso è consentito esclusivamente al personale autorizzato.

Valutazione :

Accettabile

Politica di tutela della privacy

L'Amministrazione ha messo in atto una serie di misure orientate all'adeguamento della normativa vigente nominando i dipendenti autorizzati al trattamento dei dati, ai sensi dell'articolo 2.quaterdecies del D.Lgs. 196/2003

Valutazione :

Accettabile

Gestione delle politiche di tutela della privacy

L'Ente è dotato di linee guida per l'attuazione degli obblighi introdotti dal reg. UE 679/2016 nonchè di linee guida sulla politica per la sicurezza, l'utilizzo di strumenti informatici, posta elettronica e internet.

Valutazione :

Accettabile

Rischi

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo ai sistemi.
Modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati.
La minaccia può essere utilizzata, intenzionalmente o meno, da fonti di rischio e può quindi causare un evento pericoloso.

Quali sono le fonti di rischio?

Il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato,;
Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio;
Possono essere: - un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. - un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.
Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio, Possono essere: - una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio - un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo - un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine - una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.
Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Backup, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge).

Valutazione :

Migliorabile

Piano d'azione / misure correttive :

I rischi legati ai possibili accessi illegittimi ai dati saranno di volta in volta valutati in modo da intraprendere delle misure correttive tali da garantire la sicurezza della conservazione ed integrità dei dati.

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Limitata
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?

Limitata

Rischi

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

accesso abusivo ai sistemi., Modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati. La minaccia può essere utilizzata, intenzionalmente o meno, da fonti di rischio e può quindi causare un evento pericoloso.

Quali sono le fonti di rischio?

il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato, Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio., Possono essere: - un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. - un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio. Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio, Possono essere: - una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio - un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo - un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine - una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Backup, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge).

Valutazione :

Migliorabile

Piano d'azione / misure correttive :
I rischi inerenti alle eventuali modifiche o alterazioni verranno di volta in volta valutati in modo da applicare in ogni momento misure correttive per garantire la sicurezza della gestione e del trattamenti dei dati
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? Importante
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? Trascurabile

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

accesso abusivo ai sistemi., Modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati. La minaccia può essere utilizzata, intenzionalmente o meno, da fonti di rischio e può quindi causare un evento pericoloso.

Quali sono le fonti di rischio?

il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato, Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio., Possono essere: - un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero

un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. - un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio. Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio, Possono essere: - una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio - un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo - un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine - una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Backup, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge).

Valutazione :

Migliorabile

Piano d'azione / misure correttive :
Gli eventuali rischi della perdita dei dati saranno di volta in volta valutati in modo da avere un continuo aggiornamento e miglioramento delle misure correttive a garanzia della sicurezza
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? Importante
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)?
Limitata

Panoramica

Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

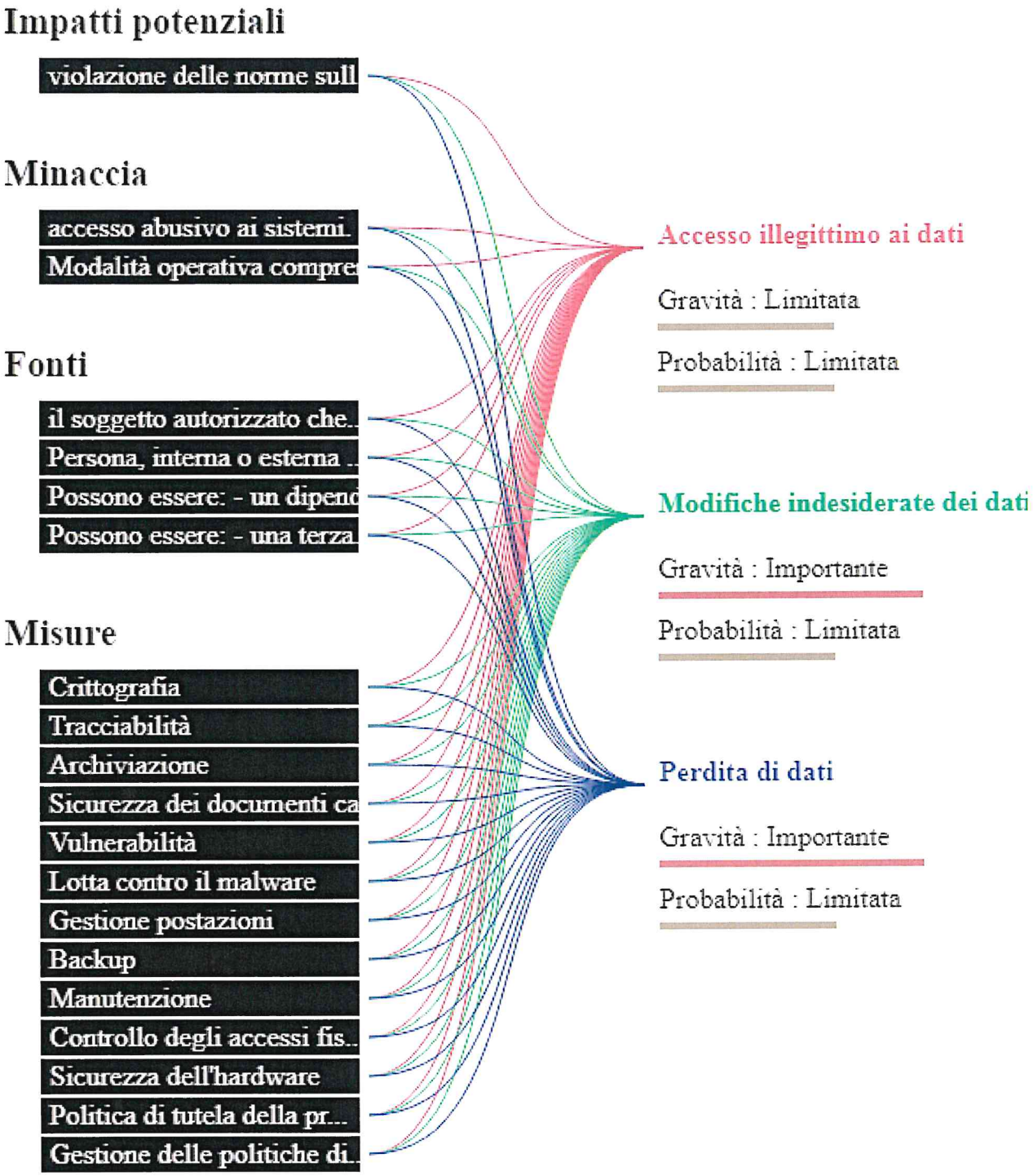
Misure esistenti o pianificate

Crittografia
Tracciabilità
Archiviazione
Sicurezza dei documenti cartacei
Vulnerabilità
Lotta contro il malware
Gestione postazioni
Backup
Manutenzione
Controllo degli accessi fisici
Sicurezza dell'hardware
Politica di tutela della privacy
Gestione delle politiche di tutela della privacy

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili


Impatti potenziali
violazione delle norme sull
Minaccia
accesso abusivo ai sistemi
Modalità operativa compre
Fonti
il soggetto autorizzato che
Persona, interna o esterna
Possono essere: - un dipend
Possono essere: - una terza
Misure
Crittografia
Tracciabilità
Archiviazione
Sicurezza dei documenti ca
Vulnerabilità
Lotta contro il malware
Gestione postazioni
Backup
Manutenzione
Controllo degli accessi fis
Sicurezza dell'hardware
Politica di tutela della pr...
Gestione delle politiche di
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Limitata
Perdita di dati
Gravità : Importante
Probabilità : Limitata

Gravità del rischio

Probabilità del rischio

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

04/04/23